BAA 04-01-MT-FH
PERSONNEL SECURITY THESIS, DISSERTATION, AND INSTITUTIONAL RESEARCH AWARDS

PROPOSER'S INFORMATION PAMPHLET

Enclosure 1

DEFENSE PERSONNEL SECURITY RESEARCH CENTER
MONTEREY, CALIFORNIA 93940-2497

Personnel Security Thesis, Dissertation, and Institutional Research Awards

For Fiscal Years 2004 - 2008

February 2004

Enclosure 1

DEFENSE PERSONNEL SECURITY RESEARCH CENTER

PERSONNEL SECURITY THESIS, DISSERTATION AND INSTITUTIONAL RESEARCH AWARDS FOR FISCAL YEARS 2004 THROUGH 2008

The Personnel Security Research Center (PERSEREC) announces the continuation of a program to help fund (through its contracting agency, the Department of the Interior, National Business Center (DOI/NBC)) research addressing issues pertinent to personnel security policy. The areas covered by this funding program include financial and credit, candidate screening and crime detection procedures, prescreening, background investigation, adjudication, continuing evaluation, employee assistance programs, security awareness, and security education. By providing financial support for master's theses, doctoral dissertations and institutional research, PERSEREC intends to respond to needs identified by the industrial and personnel security research communities and to reiterate the Department of Defense's commitment to fostering innovation within the field of personnel security.

Eligibility

We seek participation from graduate students and from scientists, faculty, consultants, and practitioners at financial, research, business, governmental, and educational institutions. To be eligible for the thesis or dissertation award, applicants must be students enrolled in a graduate program at a university accredited by the Association of Colleges and Secondary Schools for their region and be sponsored by both their university and the chair of their thesis or dissertation committee. Candidates for a master's thesis award must also have satisfactorily completed at least 2/3 of the non-thesis credit hours required for graduation in their program. To receive a dissertation award, candidates must be eligible to enter doctoral candidacy within six months from the date of their application. Prior to the dissertation award being granted, recipients must have completed all degree requirements except for the dissertation defense.

To be eligible for the institutional research award the applicants must be employees or owners of a financial, consulting, research, business, or educational institution; hold an advanced academic degree, and be sponsored by their institution.

Support

The maximum award for master's degree thesis awards is $5,000/student. The maximum award for dissertation grants is $15,000/student. The maximum award for institutional awards is $30,000/project.

Research Areas

Vetting Systems:

(Point of contact: Ralph Carney, 831-657-3002, or e-mail carneyrm@osd.pentagon.mil)

DoD personnel security vetting systems have three principle components: prescreening, a background investigation, and an adjudication that determines an individual's eligibility for a particular position. A variety of policies and procedures exist in DoD to vet individuals for employment suitability, access to classified information, suitability for other positions of trust, and reliability for handling nuclear material for weapons. Our research in this area aims to improve the effectiveness, efficiency and fairness of these personnel security vetting systems. Examples of the types of projects that would be of interest are listed below.

1) Evaluation of methods for measuring the quality of personnel security products.

2) Techniques for identifying organizational delinquents.

3) Evaluation of methods for assessing character to include loyalty, trustworthiness, and reliability.

4) Assessment of strategies to automate personnel security clearance processes.

5) Development of investigative methods that promote self-disclosure of unfavorable information.

Continuing Evaluation:

(Point of contact: Kent Crawford, 831-657-3004, or e-mail crawfoks@osd.pentagon.mil)

This area involves research aimed at helping to ensure the continued reliability, trustworthiness and loyalty of cleared personnel. We hope to systematically examine and improve three key post-vetting functions of personnel security systems: monitoring or continuing evaluation, security education, and intervention and employee assistance. Continuing evaluation includes the reporting of information that may bear on an individual's continued eligibility to hold a clearance or have access to privileged information. Security education focuses on enhancing in the minds of trusted employees an awareness of the threat and of human and technical vulnerabilities to adversaries. Finally, intervention and employee assistance looks at how security programs can help cleared individuals with personal problems seek assistance and thereby maintain their security clearance eligibility. Examples of the types of projects that would be of interest are listed below.

1) Research and development of better indicators for identifying cleared personnel who are security risks as well as the security risk associated with

particular work groups, organizations, locations, and positions. This would include the design and development of supervisory assessment forms for evaluating the security worthiness of subordinates.

2) Development and test of a taxonomy of types of motivation for different aspects of security compromise (e.g., espionage leaks, inadvertent disclosure). Determination of the implications for continuing evaluation policies and procedures of each type of compromise and motivation would also be of interest.

3) Development and evaluation of alternative strategies for gathering continuing evaluation information. This could include such approaches as self-report forms, early warning systems for identifying cleared personnel who have security-relevant problems, new continuing evaluation screening instruments, etc.

4) Development of approaches for better integrating continuing evaluation requirements with employee assistance objectives such that there is better optimization of security and human resource goals.

5) Review and assessment of incentives and constraints pertinent to the reporting of security-relevant information by co-workers and supervisors which may reflect on the suitability of a cleared employee to be entrusted with or have access to classified information. Research could assess how much resistance to reporting exists within contractor and government employee populations and why.

6) Development of improved content in security briefings and awareness training products. These products should help personnel understand and perform their security-relevant job duties as well as meet their responsibilities to protect classified information. For example, it would be of interest to know whether discussing espionage cases during training encourages or deters espionage.

7) Development of program evaluation procedures to measure the impact of security awareness programs and activities. This would include the identification of objective indicators for assessing the level of security awareness in employee populations.

8) Development of motivational enhancement techniques to promote appropriate security-relevant behavior (e.g., performance appraisal, goal setting, recognition and awards, and sanctions).

9) Assessment and testing of the relative effectiveness of various delivery systems used in security awareness programs, possibly including live briefings, computer-based modules and job aides, video presentations,

printed materials, and posters. Evaluation of delivery systems should take into consideration type of content, success at sustaining attention span, and retention of important concepts and ideas.

10) Training of those who hold security responsibilities on how to identify and deal with at-risk employees and refer them to appropriate counseling or health providers.

Automated Systems for Personnel Security:

(Point of contact: Howard Timm, 831-657-3016, or email timmhw@osd.pentagon.mil)

The primary aim of research in this area is to improve the effectiveness and efficiency of the investigative process by developing systems that electronically acquire and analyze relevant investigative data from commercial and government databases. Research that would help design or develop systems to detect and deter financial irresponsible or illegal activity is of interest. Research pertinent to automated systems that incorporate other types of individual data useful for continuing evaluation and counterintelligence purposes would also be helpful. Some examples of the type of projects that would be of interest are noted below.

1) Further validation of current financial, disciplinary, and incident-based measures, or the development and validation of new measures, for screening people on the basis of their potential for engaging in security-related offenses.

2) Identification of financial, disciplinary, or incident-based indicators that signal individuals have been engaging in serious acts of trust betrayal, such as embezzlement, theft of trade secrets, etc.

3) Creation of new financially-related security awareness and education programs, and assessment of the costs, benefits, and feasibility of modifying current employee financial assistance and counseling programs.

4) Assessment of the behavioral and financial indicators reflective of pivotal changes (improvement or deterioration) in one's level of trustworthy, reliable, and conscientious behavior.

5) Identification of information systems used by the private sector or other governmental entities for personnel security screening or offender detection that should also be utilized by the Department of Defense.

6) Identification and evaluation of commercial and government databases that could be used to help identify individuals in positions of trust having unexplained affluence.

7) Identification and evaluation of automated procedures for using large external databases to evaluate cleared personnel on a periodic basis.

Trust Betrayal

(Point of contact: Kent Crawford, 831-657-3004, or e-mail crawfoks@osd.pentagon.mil)

The research in this area is focused on understanding the phenomenon of trust betrayal, particularly espionage. There has been no shortage of journalistic and biographic writing about individual American spies and their stories. However, there is a continuing need to put these data together into an organized framework so that we can generate comparative analyses and arrive at a more comprehensive understanding of espionage and other forms of trust betrayal. This should yield information useful to security and counterintelligence policymakers as well as those responsible for security and threat awareness training and education. A recent emphasis in trust betrayal research is a focus on ensuring the continued reliability of IT personnel entrusted with the administration and control of Defense information systems. These personnel may or may not have access to classified information, but have the potential for rendering our operational systems, and the sensitive information they contain, vulnerable to adversarial interests.

1) Development of an unclassified source database containing information on Americans charged with illegally leaking information to unauthorized recipients.

2) Review of current espionage and trust betrayal deterrence practices and evaluation of the relative effectiveness of those practices in deterring potential offenders.

3) Creation of a database containing abstracts of all available personnel security research studies relating to trust betrayal, as well as a system that would enable it to be regularly updated.

4) Development of a personnel security methodology to counter computer crime by insiders.

5) Conduct single-issue studies linking trust betrayal behavior with such hypothesized causal or contributing factors as substance abuse, alcoholism, financial difficulties, or mental illness. This would include a full review of literature on the subject and case histories.

6) Creation of a source database containing information on individuals who have been prosecuted in the United States for the theft of proprietary information or critical US technology on behalf of foreign interests.

7) Creation of a source database containing information on trusted insiders with access to information systems in the United States who have been prosecuted for computer crimes including sabotage, theft of data, destruction of data or software, or the compromise of systems security.

Multidisciplinary Approaches Encouraged

Given the multidisciplinary nature of many of the research issues in this field, it may prove advantageous for the researcher(s) to seek the assistance of those working in other disciplines (e.g., business, industrial psychology, criminal justice, law, etc.). Doctoral students also should consider whether their dissertation committees would be enhanced by having one or more members from a different department. Similarly, principal investigators applying for an institutional award should consider whether their ability to address their research questions would be improved by consultation or collaboration with experts from other fields. The primary considerations for assessing whether a multidisciplinary approach is warranted are the type of questions to be addressed and the scope of the researcher's expertise.

Preparation and Submission of Proposals

The personnel security thesis, dissertation and institutional research award programs are competitive. Only a limited number of awards in each category can be awarded each year. Proposals that would help increase the efficiency or effectiveness of personnel security programs, lead to implementable recommendations, and establish empirically based findings using subject populations that are generalizable to those found in the industrial, military, or civilian government sectors are especially encouraged.

The proposals must be self-contained (no videos, please) and no longer than 25 pages excluding curriculum vitae. The proposal should include the informational statements described below. An original, signed by an official authorized to commit the institution contractually, and three copies must be submitted. If possible, use the following format.

1. ***Title Page***. The title page should include the following information in the order indicated:
    a. Name and address of the institution
    b. Title of the proposal
    c. A notation whether the proposal is submitted to the "Personnel Security Thesis Research Award Program," the "Personnel Security Dissertation Research Award Program," or the "Personnel Security Research Institutional Award Program"
    d. The research area (e.g., clearance processes, continuing evaluation, financial and credit, etc.) under which the proposal falls
    e. Name, title, address, phone number, and email address of the principal investigator (i.e., the graduate student for the master’s thesis and dissertation award proposals or the lead researcher for the institutional award proposals)

f. Names and telephone numbers of business personnel to be contacted for award negotiation

g. Names, titles, and signatures of official(s) authorized to obligate the institution

h. Date of submission

i. Proposed start and end dates

j. Identification of any proprietary information to be used by DOI/NBC for evaluation purposes only (the data which the author wishes to restrict should be marked with a legend in accordance with Federal Acquisition Regulation 52.215-12)

2. ***Proposal Narrative***. The narrative of the proposal should include the following items.

   a. Statement of the problem and its importance

   b. A section describing how the proposed research relates to the personnel security issues

   c. Evidence that the literature has been reviewed

   d. Specific research questions to be explored

   e. Description of the methods, including data collection and analysis methods

   f. Time schedule for the major events of the study

   g. Anticipated policy and program implications of the findings for the field of personnel security

   h. Documentation to the effect that the needed cooperation from organizations will be forthcoming

   i. A clear, concise listing of project deliverables (e.g., technical report, copy of data, software, etc.)

3. ***Budget.*** A comprehensive estimated budget must be included that falls within the upper limits of the support possible under the applicable award program delineated in this announcement. The budget should cover all categories of expense that will be incurred during the course of the project, including: 1) salary cost, 2) overhead or burden rates, 3) supplies and materials, 4) equipment, 5) travel costs, 6) report preparation costs, 7) consultant or sub-award costs, 8) communication costs, 9) computer expenses, 10) other direct costs, and 11) total costs. Cost sharing and matching funds to be provided by the applicant's institution and by other sources should be noted.

4. ***Thesis or Dissertation Committee Chair's Statement*** (Thesis and dissertation award programs only). This statement should indicate the thesis or dissertation committee chair's support of the proposal and the chair's evaluation of the interests

and potential of the candidate. The chair should also include a brief description of the backgrounds of the other members of the thesis or dissertation committee.

5. ***Description of the Researcher(s)'s Background***. The proposal must be accompanied by evidence of the background of the researcher(s). This evidence will include information on the education, employment experience, and publications of the researcher(s). Normally, this requirement will be met by the inclusion of the curriculum vitae of the investigators. Proposals submitted under either the thesis or dissertation award program should include the curriculum vitae of the thesis or dissertation committee chair and a statement noting whether the candidate has met all requirements for the degree, other than the thesis or dissertation, and, if not, when those requirements will be met.

Selection Criteria

The selection criteria that will be used to evaluate the proposals will be:

1. The perceived need for the subject matter in the personnel security body of knowledge. Will the study help to resolve questions that would be of use for improving the field of personnel security?

2. Practical applicability of results. Are the topic and the study design such that the results of the research may have direct implications in the development and implementation of policy in the area of personnel security?

3. Strength of the evidence showing that the applicant(s) possesses the necessary qualifications to produce an acceptable research product. Is the proposal clearly written? Does it include essential details that enable the reviewer to conceptualize the project in its entirety? Does the proposal indicate that the researcher(s) has/have knowledge of the significant literature? Does the proposal contain the essential elements of a well-developed research plan? Do the curriculum vitae reflect a track record of research accomplishment or potential?

4. Quality and feasibility of the research methods. Is the methodology suited to the kind of study proposed? Does the plan indicate that the appropriate information will be collected? Is there evidence that the capacity exists for properly analyzing the data that will be collected?

5. Originality of the research. The originality may apply to the topic itself, or to the treatment of a topic that has already been the subject of considerable research.

6. Realism and reasonableness of the estimated expenses. Have all of the likely expenses been included? Are the project expenses both realistic and reasonable? To what extent is the institution providing support through cost-sharing measures?

When and Where to Submit

Proposals based on this announcement may be submitted, and will be accepted, any time through 4:00 P.M. MST, 30 September 2008. PERSEREC will, on a regularly scheduled continuing basis, evaluate and fund, through DOI/NBC, selected proposals received during the open period. Proposals should be sent to the following address:

Department of the Interior
National Business Center
Acquisition & Property Management Division, Southwest Branch
Attention: L. Carter
PO Box 12924
Ft. Huachuca, AZ 85670-2924

For FEDEX deliveries, proposals should be sent to the following address:

Department of the Interior
National Business Center
Acquisition & Property Management Division, Southwest Branch
Attention: L. Carter
Building 22208, 2nd Floor, Auger Street
Fort Huachuca, AZ 85613

Additional Information

Telephone, mail, and electronic mail inquiries about the Personnel Security Research Programs are welcome. Inquiries related to research issues should be directed to:

Director,
Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
ATTN: BAA 04-01-MT-FH (L. Lewis)
Monterey, CA 93940-2497
Tel: (831) 657-3000
FAX (831) 657-0153
perserec@osd.pentagon.mil

Inquiries related to administrative or contractual issues should be directed to:

Lawrence H. Carter
Department of the Interior
National Business Center
Acquisition & Property Management Division, Southwest Branch
PO Box 12924
Ft. Huachuca, AZ 85670-2924
Lawrence_H_Carter@nbc.gov